REMARKS

Claims 1-32 are pending. Claims 1-32 are rejected. Claims 1, 5, 6 and 19, 24-27 and 29-32 are amended. This Response is filed in reply to the Office Action dated September 30, 2004.

Amendments to the claims are not an acquiescence to any of the rejections. Furthermore, silence with regard to any of the Examiner's rejections is not an acquiescence to such rejections. Specifically, silence with regard to Examiner's rejection of a dependent claim, when such claim depends from an independent claim that Applicant considers allowable for reasons provided herein, is not an acquiescence to such rejection of the dependent claim(s), but rather a recognition by Applicant that such previously lodged rejection is moot based on Applicant's remarks and/or amendments relative to the independent claims (that Applicant considers allowable) from which the dependent claim(s) depends. Applicant reserves the option to further prosecute the same or similar claims in the instant or a subsequent application. Upon entry of the Amendment, claims 1-32 are pending in the present application.

The issues of the subject Office Action are presented below with reference to paragraph markings of the Office Action:

With regard to the Office Action, paragraphs entitled "Claim Rejections - 35 U.S.C. §112:" The Examiner stated that there is insufficient antecedent basis for the limitations "MODE field" in claim 21 and "using 3GPP (Third Generation Project Partners) AKA (authentication and key agreement)" in claim 32.

With regard to the Office Action, paragraphs entitled "Claim Rejections - 35 U.S.C. §102:" The Examiner rejected claims 19-26, 30 and 31 under 35 U.S.C. §102(e) as being anticipated by Aura, U.S. Patent Ser. No. 6,711,400 (referred to hereinafter as Aura).

With regard to the Office Action, paragraphs entitled "Claim Rejections - 35 U.S.C. §103:" The Examiner rejected claims 1-18 and 27-29 under 35 U.S.C. §103(a) as being unpatentable over Aura in view of Marshall et al., U.S. Patent Ser. No. 4,888,800 (referred to hereinafter as Marshall). The Examiner rejected claim 32 under 35 U.S.C.

§103(a) as being unpatentable over Aura in view of Marshall et al., and further in view of Maupin, U.S. Patent Ser. No. 6,600,917 (referred to hereinafter as Maupin).

Applicant traverses the Examiner's rejections under 35 U.S.C. §112, 35 U.S.C. §102(e) and 35 U.S.C. §103(a), and respectfully requests reconsideration in view of the amendments and remarks.

Claim 21 depends from claim 20 and recites that the identification (as received in claim 20) "comprises a value of a MODE field." (emphasis added) As is standard practice in claim drafting, the use of the article "a" is appropriate for a first use of the respective terms "value" and "MODE field". The term "a MODE field" does not imply reference to a preceding "MODE field" term, so does not require antecedent basis. Claim 32 recites the use of "3GPP (Third Generation Project Partners) AKA (authentication and key agreement)" for handling authentication and key agreement between the mobile station and the service network if it is determined that the home environment and the service network do not share a cryptographic primitive. As recited in claim 32, the term "3GPP (Third Generation Project Partners) AKA (authentication and key agreement)" does not imply reference to a preceding "3GPP AKA" term, so does not require antecedent basis. Applicant requests reconsideration of the rejection of claims 21 and 32 under 35 U.S.C. §112 in light of the above. Alternatively, Applicant respectfully requests clarification of the rejection if the rejection has been misunderstood.

Aura describes a method in which individual authentication processes are accomplished between a mobile station and an authentication center. The reliability of the network is checked in connection with every authentication, and the information transferred between the network elements is insufficient to make it possible to use a false identity.

Applicant recites techniques that can enable authentication and/or key agreement between communications network stations and service networks. The techniques can include the negotiation and use of a cryptographic primitive that can be shared between a service network and a home environment of a station. The techniques can also feature a

key usage indicator, such as a sequence number, that can be maintained by the service network and a station. Comparison of the key usage indicators can, for example, permit efficient authentication of the service network.

With respect to claim 1, Applicant agrees with the Examiner that Aura does not disclose adjusting a value corresponding to key usage. While Marshall discloses a counter in association with the usage of an encryption key, Marshall does not teach or suggest that the counter or *verification value forms a part of a verification computation enabling the station to authenticate the service network*, as recited in Applicant's claim 1. As described in Marshall, the counter provides a determination of usage such that the User Master Key (UMK) can be changed after sufficient usage (col. 7, lines 19-27). In Marshall, it is the Key Distribution Center (KDC) that provides new keys to the terminals. Marshall does not teach or suggest that information corresponding to the verification value is transmitted from the service network to the station. Contrary to the Examiner's assertion, transporting a new key value to the terminals by the KDC does not correspond to transmitting information corresponding to the verification value from the service network to the station.

The Examiner notes that the implementation of the usage counter as taught in Marshall in the method of Aura would provide means for updating the encryption key. However, Applicant's adjusting of the verification value is used in authenticating the · service network to the station and does not update the key stored at the service network. · Thus, even the implementation contemplated by the Examiner fails to teach or suggest the elements of claim 1. Claim 12 recites elements similar to claim 1 in that the station and service network maintain key usage indicators, the station receives the key usage indicator maintained by the service network, and compares the usage indicators to authenticate the service network. Based on the above reasoning with respect to claim 1, Marshall does not teach or suggest receiving at a first terminal (or station) a usage counter from a second terminal (or service network) and comparing the usage counters of the two terminals to authenticate the second terminal to the first terminal.

Since Aura and Marshall, alone or in combination, fail to teach or suggest all of the elements of claims 1 and 12, it follows that claims 1 and 12 are patentable over Aura in view of Marshall. Reconsideration of the rejection and allowance of claims 1 and 12 are respectfully requested. Claims 2-11 and 13-19 depend from claims 1 and 12, respectively, and are allowable at least by dependency.

With respect to claim 19, Applicant recites that the home environment determines *a cryptographic primitive offered to the home environment by the service network*. The Examiner asserted that Aura implies (Fig. 3) that the home network is aware of the primitive used at the base station. However, Aura does not teach or suggest in the description of Fig. 3, or in Fig. 3 itself, that a cryptographic primitive is offered by the service network. In fact, the only communication from the service network to the home environment described in Aura is the transfer of the station's IMSI and RAND1 variables to the home environment. Since the service network merely passes these variables to the home network, the service network cannot be said to offer a cryptographic primitive to the home environment, much less receive identification of the cryptographic primitive in the value of a MODE field. As can be clearly seen from the Examiner's assertions with respect to claims 20 and 21, the Examiner appears to confuse the offering of the cryptographic primitive to the home environment (or the receipt of the cryptographic primitive, as recited in claims 20 and 21) with the transfer of RAND2 or SRES1 to the station from the home environment. Based on the above, Aura does not anticipate claim 19. Reconsideration of the rejection of claim 19 and allowance of claim 19 are respectfully requested. Claims 20-23 depend from claim 19 and are allowable at least by dependency.

With respect to claim 24, Applicant recites *storing different sets of cryptographic information for different respective service networks*. The Examiner asserts that Aura discloses storing different sets of cryptographic information in that the computed DCK is used in conjunction with a particular visiting network BS. However, since the DCK is computed for each particular network, the station does not store sets of cryptographic information for different service networks, but rather stores the DCK for one particular

network when communicating with that network. When communicating with a different service network, a new DCK is computed for that service network. No other DCK's or sets of DCK's are stored. Since Aura does not store sets of cryptographic information, it follows that Aura cannot select one set from among the sets to communicate with the one service network for which the set was selected.

Based on the above, Aura does not anticipate claim 24. Reconsideration of the rejection of claim 24 and allowance of claim 24 are respectfully requested. Claims 25-31 depend from claim 24 and are allowable at least by dependency. In addition, claims 27-29 recite that the sets include indicators of usage. For the reasons previously provided with respect to claims 1 and 12, claims 27-29 are deemed separately allowable.

With respect to claim 32, Applicant recites a method including *determining whether the home environment and the service network share a cryptographic primitive offered by the service network.* For the reasons provided with respect to claim 19, Aura does not teach or suggest such a determination. Additionally, as described by Aura, the method of Fig. 3 cannot guarantee that the base station, which the mobile station is connecting to, is reliable (col. 5, lines 13-15). Thus, Aura teaches away from the use of the prior art methods (Figs. 2 and 3) asserted by the Examiner to disclose the shared primitive recited by Applicant. Instead, Aura describes the use of a method (Fig. 4) where the service network and mobile station do not share algorithms. Rather than the use of a shared algorithm, the service network compares a variable (SRES2') forwarded by the home environment to a variable (SRES2) forwarded by the mobile station. If the two variables are equal the service network uses a key Kc, also forwarded by the home environment, for communication with the mobile station.

Claim 32 recites that the use of the key K shared by the home environment network and mobile station in the 3GPP AKA is replaced with the shared secret key (SSK) when the home environment and the service network share a cryptographic primitive. Aura in Fig. 3, does not teach a shared secret key K. Nor does Aura, in Fig. 4 teach a shared cryptographic primitive. Maupin describes a network wherein base

FHBOSTON/1123739.1

-12-

stations broadcast capabilities messages to advise mobile stations of the services supported by the base stations. Maupin does not specifically teach cryptographic techniques for network communications and does not describe the use of 3GPP AKA. Particularly, Maupin does not teach replacing the use of K with SSK. Thus, the combination of Aura and Maupin does not teach or suggest all of the elements of Applicant's claim 32 and claim 32 is thus patentable over Aura in view of Maupin.

Based on the distinctions described herein between the cited references and Applicant's independent claims, Applicant respectfully suggests that Aura does not anticipate Applicant's claims 19-26, 30 and 31. Further, for the reasons cited above, Applicant's claims 1-18, 27-29 and 32 are patentable over Aura in view of Marshall and/or Maupin. Reconsideration of the rejections of the claims under 35 U.S.C. 102(e) and 103(a) is respectfully requested.

The remarks herein should in no way be construed to be an acquiescence to any of the rejections. The remarks herein are being made solely to expedite the prosecution of the above-identified application. Applicant reserves the option to further prosecute the same or similar claims in the instant or subsequent patent applications.

FHBOSTON/1123739.1

-13-

Serial No. 09/710,541
Atty Dkt: 99-956

CONCLUSION

Based on the above amendments and remarks, it is respectfully submitted that the claims and thus this application are in condition for allowance. Accordingly, reconsideration and allowance are requested. If there are any remaining issues or the Examiner believes that a telephone conversation with Applicant's attorney would be helpful in expediting the prosecution of this application, the Examiner is invited to call the undersigned at (972) 718-4800.

Respectfully submitted,

Date: December 28, 2004

_____
Joel Wall
Attorney for Applicant
Registration No. 25,648

Verizon Corporate Services Group Inc.
c/o Christian Andersen
600 Hidden Ridge, HQE03H14
Irving, TX 75038
Tel: (972) 718-4800
CUSTOMER NO. 32127

FHBOSTON/1123739.1

-14-